Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 00 (2014) 000–000

Procedia Technology

www.elsevier.com/locate/procedia

CENTERIS 2014 - Conference on ENTERprise Information Systems / ProjMAN 2014 - International Conference on Project MANagement / HCIST 2014 - International Conference on Health and Social Care Information Systems and Technologies

Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging

Iryna Yevseyeva[a]*, Charles Morisset[a], James Turland[a], Lynne Coventry[b], Thomas Groß[a], Christopher Laing [c], Aad van Moorsel[a]

[a] *Centre for Cybercrime and Computer Security, School of Computing Science, Newcastle University, Newcastle-upon-Tyne, NE1 7RU, United Kingdom*

[b] *Psychology and Communication Technology Laboratory, School of Health & Life Sciences, Northumbria University, Newcastle-upon-Tyne, NE1 8ST, United Kingdom*

[c] *Faculty of Engineering and Environment, Department of Computer Science, Northumbria University, Newcastle-upon-Tyne, NE1 8ST, United Kingdom*

Abstract

In this work we address the main issues of IT consumerisation that are related to security risks, and propose a 'soft' mitigation strategy for user actions based on nudging, widely applied to health and social behaviour influence. In particular, we propose a complementary, less strict, more flexible Information Security policies, based on risk assessment of device vulnerabilities and threats to corporate data and devices, combined with a strategy of influencing security behaviour by nudging. We argue that nudging, by taking into account the context of the decision-making environment, and the fact that the employee may be in better position to make a more appropriate decision, may be more suitable than strict policies in situations of uncertainty of security-related decisions.

Peer-review under responsibility of the Organizing Committees of CENTERIS/ProjMAN/HCIST 2014

Keywords: consumerisation; security; risks; mitigation strategies; nudging

* Corresponding author. Tel.: +44-191-208-7873; fax: +44-191-208-8232.
E-mail address: iryna.yevseyeva@newcastle.ac.uk

Peer-review under responsibility of the Organizing Committees of CENTERIS/ProjMAN/HCIST 2014.

1. Introduction to consumerisation of IT

Globalization and the worldwide availability of the Internet (for both stationary and mobile devices) has led to the elimination of the spatial divide within traditional working environments, and thereby enabling the working environment to be highly mobile. Increasingly, people work not from a single office, but from multiple offices, on customer sites, when traveling, at home and in public places. At the same time, the technology markets fuel and adapt to such dynamic environments by regularly supplying a variety of new mobile devices to meet different business requirements and purposes.

The rapid development of IT products and their constantly reducing costs make the best "high-tech" technologies available not only to large companies, but also to the general public for personal usage. Data interchange is also increasing. Storing data on individual devices not only becomes impractical, but also insufficient for its distributed usage. Cloud-based solutions are therefore of high demand for both private and work-related usage by employees.

This orientation of products and services towards the user is known as *consumerisation of IT*. Here, a user (an employee of a company) is also a consumer of devices and services, both owned by the company (the user's employer) and privately purchased by the user. The use of such products and services via the Internet for personal activities (e.g. social networks and other web tools) pushes companies to adapt business technologies used by employees for personal purposes. At the same time, companies expect an employee to be productive and responsive at anytime from anywhere, thus integrating employees' personal life with their work. In turn, companies that keep pace with new technologies and take full advantage of them have more chances to improve their business and both short- and long-term returns [1].

Under the conditions of a fast growing economy and improved technologies, such "mobilization" of businesses will continue, involving further companies and employees. To stay competitive in such a dynamic market, companies need to quickly adapt to these trends and provide their employees with ways of working in such mobile environments, for instance by providing them with up-to-date mobile phones, laptops and/or tablets. However, frequently updating the equipment of employees is costly for companies and the pace of upgrades may not keep up with their expectations.

In such circumstances, a recent trend is for companies, large firms and *small to medium enterprises* (SMEs) alike, to allow their employees to work with their own devices. This strategy, known as *bring your own device* (BYOD), introduces flexibility for employees and affords the opportunity for the companies to satisfy the wishes of their employees to work with devices they own without increasing equipment budgets.

Many practitioners consider further IT consumerisation inevitable. Trend Micro Inc. performed a survey confirming that 74% of IT enterprises were allowing BYOD for their employees. However, they emphasized that consumerisation of IT carries strategic and operational challenges and *'creates security risk, financial exposure and a management nightmare for IT*' without a planned approach to it [2].

Together with opportunities consumerisation of IT introduces some severe security risks. These risks include: weak control over employees private devices (e.g., old or absent anti-virus software); possible weakness of protection measures of services used to transfer or store company data; potentially unsecure environments, in which employees may use their mobile devices (e.g., public places or foreign countries).

In addition to preoccupations related to technical security aspects, human factors are of high importance in the context of global consumerisation. On the one hand, when using personal devices for work (or company devices for personal purposes), the border between personal and company data becomes blurred. On the other hand, attempts from companies to take control over personal devices for their better protection may meet opposition from employees, and disturb their ownership perception associated with their devices and privacy intrusion sentiments. Therefore, companies must consider these facts when developing their security policies.

In this work we consider how changes in the employees working context (from the office to public places or home) and in the ownership of the devices (from corporate to personal) introduce uncertainty in security decisions. We suggest a 'soft' strategy to assist in security decision-making under uncertainty, based on nudging. This approach was defined for health and social solutions [3,4] and recently studied in the context of security and privacy decision-making [5-11]. In particular, we indicate when nudging may be beneficial to both the company and employee and, consequently, lead to a more secure and productive society in general.

In Section 2, we discuss practical approaches to risk assessment and mitigation of consumerisation risks existing in the literature. In Section 3 we analyse in more detail the uncertainty that consumerisation of IT brings to security decisions and provide an approach to influence the behaviour of users towards more secure or more productive choices based on nudging techniques widely applied in marketing. Finally, we conclude this work and outline the direction of future research in Section 4.

2. Approaches to consumerisation risk assessment

Different organizations may have different risk assessment strategies and may include in their security policy only risks specific to their activity. The European Network and Information Security Agency (ENISA), which develops security recommendations for EU countries, delivered a report that may serve as a good guideline for SMEs to perform a risk assessment [12]. According to this report, a company should identify its *risk profile* depending on the: size of the company; yearly revenue; data type a company is dealing with (e.g. critical personal data, such as medical information, customer data or just employees data); and loss of reputation and customers confidence depending on unavailability of service. The critical *assets* should be identified among systems (server, laptops, workstations storage, archiving and backups), network (routers, cabling, gateways wireless access points, network segments, etc.), people (HR, R&D, Sales and Marketing, Contractors and Third Party, Operations and Technology) and applications (ERP, Logistics, e-commerce, financial control, logistics) categories. In particular, for each asset the security requirements related to the confidentiality, integrity and availability aspects should be identified.

Depending on the company risk profile and critical assets, ENISA suggests selecting a number of organizational and asset-based controls that will become a part of a security requirements list, implemented within either physical security, system and network management, system administration tools, monitoring and auditing IT security, authentication and authorization, vulnerability management, encryption, security architecture, incident management or general staff practices [12]. The identified key security areas of the company help to shape its security efforts, in particular (i) defining and selecting requirements to be implemented within company's security policy; (ii) specifying key technical and management controls for preventing disasters and incidents; (iii) developing recovery plans and educational programs needed for staff training.

In addition to standard risk assessment, e.g. based on ENISA proposed scheme [12] or ISO/IEC 27005:2011 [13], when assessing the BYOD strategy of a company, opportunities should be considered. ENISA analysed IT consumerisation considering related costs and opportunities [14], and suggested various mitigation strategies to reduce the risks in the areas of *governance*, *legal and regulatory issues* and *technical issues* [15], which are related to potential losses and gains that a company may have with respect to confidentiality, integrity or availability of its assets when introducing IT consumerisation. These mitigation strategies correlate with concerns related to consumerisation reported by several Chief Information Security Officers (CISOs) of large enterprises interviewed by Microsoft [16], such as *governance* related to monitoring of personal devices, *e-discovery* associated with legal issues of business data stored on personal devices, and *general security and control of data* for privately owned devices.

MWR Security published a detailed report on mobile devices security, including BYOD strategies for companies, in cooperation with the Centre for the Protection of National Infrastructure (CPNI) [17]. According to this report, companies developing a security policy including mobile devices and BYOD strategy should consider the following challenges: (i) fast developing IT technologies in general and the constantly emerging variety of mobile devices in particular; (ii) different risk profiles within variety of vendors of the same type of device (for instance, iPhone-based and Android-based mobile phones risk profiles are different, moreover, risks vary between devices using different versions of the same Operating System (OS)); (iii) *assets* that a company possesses and tries to protect; (iv) possible assets *vulnerabilities* (which are assets weaknesses that can be used for security breaches); (v) *threats* (against what the protection efforts are directed) and *risks* specific to the activities of the company and its employees; (vi) variety of working locations, both public (cafes, parks, hospitals, organizations) and private (home, other companies); (vii) organizational structure, whether it is an SME (with mainly 3rd party vendors/suppliers taking care of security) or a large company (with a CISO dedicated to maintaining company security).

In addition to technical challenges, attention should be paid to user awareness of risks, their education and advising or providing recommendation to user whenever possible [17]. Employers may consider different educational tools for teaching their employees the security issues related to their company's policy, and promote a security culture, e.g., with rewards for secure behaviour. However, these are long-terms approaches, require time and involve user awareness and conscious decision-making. While users may be aware and intend to behave securely, these intentions do not always translate into actual behaviour. Therefore a complementary alternative approach would be to try to influence the behaviour of the decision makers directly at the moment of the decision-making.

Influencing user behaviour instead of forcing it looks very attractive for security decisions in situations of uncertainty that may be related to dynamic contexts, in which user may 'know better', and/or to dealing with mobile devices, which employees use, but which are not fully controlled by the company-employer. In the next section we will explore an influencing approach in security.

3. Assistance in risk assessment under uncertainty

We now propose an approach to risk assessment assistance in situations of uncertainty. The standard risk assessment procedure, for instance suggested in [12] or [13], is adjusted taking into account consumerisation of IT adaptation, e.g. proposed in [15], and includes: the estimation of company activities profile; the corporate data and the evaluation of the vulnerabilities and threats of professional or personal devices; the security checks of services employees use on a daily basis; and the analysis of potential human behaviour vulnerabilities. Moreover, we consider the *ownership* of devices and data (private or corporate) as well as the *context,* in which the devices, services and data are used. Here, by context, we mean a dynamic environment, e.g. work, home or a public place, in which the mobile device users may use devices or data or services. Note that the context may include services that the employee is allowed to use, e.g., owned by company, bought by employee or freeware.

3.1. Risk assessment for consumerisation of IT

The designer of a security policy for a company working with mobile devices should consider the properties given in Table 1. Together with important functionalities, they may expose security vulnerabilities of devices. Paradoxically, one of the greatest advantages of mobile devices, mobility, is also one of its greatest vulnerabilities. Some devices types (laptop and tablet) have large screen, which makes them convenient for regular tasks (e.g., writing/reading emails, programming, watching video), but it also becomes easier to shoulder surf these devices and data shown on large screens be disclosed. In Table 1 '+', '-' and '?' refer to the vulnerability of the device type present, absent, or not always present in it, respectively.

Table 1. Vulnerabilities of devices

Property	Laptop	Tablet	Phone	USB Stick
Connectivity	+	+	+	+
Mobility	+	+	+	+
Applications	+	+	+	+
Lock	+	+	+	?
Remote Access	+	+	+	+
Out of date software/OS	+	+	+	+
Large screen	+	+	-	-
Admin access	+	?	?	-
Removable Media	?	+	+	-
Access to SIM card	?	?	+	-

Here, we refer to a *private device* as a mobile device bought by an employee and to a *corporate device* as a mobile device bought by a company for an employee to work on. Then, a *mixed-usage device* is a private device

used not only for personal, but also for working purposes or corporate device used for not only working purposes but also personal ones.

Table 2 presents an example of threats adapted from [17] to mixed-usage devices, taking into account vulnerabilities presented in Table 1 and considering possible scenarios in which an employee may happen to work.

On the one hand, many threats presented in Table 2 can be controlled with technical solutions, such as *data loss/leakage prevention* (DLP), if private devices are locked down in a similar way as corporate devices with some security policy and/or with *mobile device management* (MDM) programs that allow management of the assets (both devices and data). Practitioners consider MDM as a necessary risk prevention tool [18], and urged for the need for an MDM version for Android-based devices [19] for companies adopting IT consumerisation. The help of mobile *Virtual Private Network* (VPN), which extend private network across a (various) public networks, was already appreciated by companies with 'mobile' employees and Research in Motion (RIM) announced a multi-platform version of its BlackBerry Enterprise Server [19] for improving security of mobile devices. Separation of private and corporate data with data segregation tools may help to differentiate data to be monitored/filtered or not.

On the other hand, many threats presented in Table 2 involve risk prone actions, which increase security breaches significantly. Hence, company's security policies efforts are twofold: the identification of technical controls to apply (e.g., which anti-virus to buy, which software to install and how to control its updates, which ways to access corporate data are allowed and how to guarantee data protection); and the prevention of possible human errors, with technical controls when possible, such as control over anything installed by the user and password creation rules, or with education sessions, for instance on not sharing personal credential, public Wi-Fi connection and policy jailbreaking.

Table 2. Threats for devices and corporate data

Device compromised	Device contaminated	Communication compromised	Data compromised	Data disclosed	Security / trust model weakened
Device lost	Malicious application installed by user	Data interception in transit	Integrity (access via security breach)	Inappropriately stored / transferred data	Personal credentials shared
Device stolen	Device infected by malware / virus	Encryption key disclosed	Confidentiality (access via security breach)	Discloses data after being asked (social engineering)	Device jailbroken
Device decommissioned	Device contamination	Insecure unencrypted connection	Availability (denial of service)	Discloses data unintentionally (shoulder surfing/ duplication)	Security controls bypassed

Risk is usually considered as the likelihood of an attack multiplied by its impact, where the likelihood of an attack is given by the probability that a threat can exploit a particular vulnerability. A typical approach to reduce risk is therefore to add some *control* over the vulnerabilities, so that they are no longer exploitable. However, the usage of mixed-usage devices raises the problem of who is responsible to apply some control. Here, *control* refers to 'a measure that is modifying risk' [13].

Table 3. Control of devices depending on ownership and manager

		Device Manager	
		Company	Employee
Device Owner	Company	(1) Full control	(2) Partial control
	Employee	(3) Partial control	(4) No control

Moreover, we differentiate between different levels of control that may maximally reduce risk with *full control* over devices; *partially* control devices or have *no control* over devices. Table 3 adapted from [17] shows four possible cases of combination of a device owner and a device manager: 1) when company provides employees with devices and takes full control of these devices, e.g. typical BlackBerry 'work phone'; 2) company provides devices, but not manage them, e.g. common for universities, having partial control over the devices; 3) own devices of employees are controlled by companies partially, e.g. iPads and iPhones can be registered to be wiped in case of loss; 4) employees are allowed to work with their own devices, but have to take care of security themselves, resulting in company having no control over the devices.

The first case (1) is the case of full control: a company both owns and manages the device. Depending on how restrictive the security policy is and how well it is complied with, there are still possible threats and corresponding risk to the assets of the company, e.g., zero-day vulnerabilities. In case (2) a company provides devices, but does not manage them, or in case (3) employees use their own devices, and either company manages them as in case (3) or not as in case (4). In cases (2) and (3), a company may apply some security policy to protect the employee's personal or corporate devices with DLP and/or MDM tools. In case (4), there is a danger of uncontrolled threats, as an employee might not use some or any protection measures, such as an anti-virus, software updates, passwords, etc.

3.2. Nudging for mitigating security risks and improving productivity

Security policy should be seen as a protective measure, which employees should comply with. In addition to punishments for risky behaviour and rewards for secure ones, it should take into account employees' perspective on security rather than strengthening the security strategy. A highly restrictive security policy that limits flexibility of employees might result in a rebellion effect and push employees towards overriding it. Fundamentally, it would expose the company to security risks and corresponding costs related to legal issues that should be taken into account when developing a security policy. The problem of non-compliance with security policy even when knowing about possible risks was studied earlier, and it was shown that there is some compliance limit for each user (probably, varying from user to user), *compliance budget* [20]. Further research [21] focused on understanding non-compliance and workaround strategies employees apply in order to be more productive and perform their tasks faster.

Moreover, too restrictive security policies may be less flexible to the dynamic context, in which security decisions are made. For instance, a security policy of a company allows its employees to connect only to Wi-Fi's in the whitelist of a company. However, there may be no available white-listed Wi-Fi's at the meeting site an employee is attending. Hence, the only option for an employee to work would be to connect to a publicly available Wi-Fi. Often at the moment of making security decisions there is no objective information for evaluating consequences of each possible choice, and often such decisions are made in situations of uncertainty. For instance, when connecting to a non-secure public Wi-Fi the decision makers might not realize the risks and consequences of possible security breaches. However, the choices still should be made (e.g. one of the Wi-Fi's should be selected for work) and the decision maker should take responsibility for (even unrecognized) consequences of such decisions.

The traditional approach for helping employees to make better security decisions is via education and training sessions on the security policy of the company [15,17]. It is an efficient, but time-consuming approach that requires conscious reflection of employees on security issues and possible consequences of such decisions for them and their company. Contrary to education on security risks, nudging is an explicit recommendation or more subtle influence emphasizing some choice, but not forcing it. It has a reputation of making a big difference by small changes and still leaving the freedom of choice to the decision maker, who might require it when working on his/her own device. It is also important when security decisions are made in situation of uncertainty, where an employee might be better informed than the company, possessing more information on the context of the decision.

3.2.1. Nudging for security and productivity: What is it?

In this work, we investigate a possibility to apply a recently proposed '*nudging*' approach [22] to influence information security choices as a 'soft' alternative to more restrictive security policy that would leave no choice to decision makers. Nudging provides a framework, called *choice architecture*, which presents available alternatives in

such a way that influences the decision makers' final choice [22]. This approach is libertarian paternalist in nature, according to which in the health and social behaviour domains 'people are free to do what they choose, but that it is legitimate to influence people's behaviour in the positive health direction' [23]. Ability to influence behaviour of populations is appealing to governments as they wish to improve health of their nations but still be seen to provide freedom of choice, i.e. people can opt out.

Nudging has been widely used in healthcare [3] and social policies [4] to change behaviour of people with minimal interventions. In these initiatives the nudged behaviour is widely accepted as the best according to both governments and population, such as fighting obesity of children and returning debts by taxpayers, respectively. The research results on applied cases of nudging are very encouraging and show that, indeed, the manner, in which the information is presented to the decision maker, influences the choice. For instance, it was shown that rearranging menu items in student's cafeteria may increase/decrease consumption of a particular item by up to 25%, since the first options in the list have higher chances to be selected [22].

Similarly, the nudging can be adapted to influence people's choices in information security. The solutions towards which nudging will be done should be based on rigorous models developed using quantitative risk assessment techniques. They should take into account the trade offs between productivity benefits and security risks for each particular scenario, and nudge the decision maker towards the best compromise trade-off solutions, but also taking into account context of the decision-making, security policy of the company and preferences of the particular decision maker when possible. Assuming that uncertainty is present in such security scenarios, the outcome of the rigorously assessed models will be used to frame choice architecture for decision makers in such a way that it nudges decision-makers to make better information security and productivity decisions, but still leaves the final choice for the decision maker.

Nudging towards more secure and/or more productive solution(s) may be seen as improving security for society or advice from an employer to a hesitating or not aware of danger employee. Nudged users may either 'fall' into the nudge or ignore it, if it does not look appealing. Such an approach leaves the final choice with an employee; this assumes that they understand what is better for him/her in the context of the decision-making, but puts all responsibility for the final choice on the decision maker.

3.2.2. Nudging for security and productivity: How to influence?

Six influencing techniques are presented in [22]: incentives, understanding mapping, defaults, give feedback, expect error and structure complex choices when creating *nudges.* They can be used to build a choice architecture that aims to influence choice made by the decision maker.

To develop *incentives* for information security, we need to understand the rewards that would encourage employees to make the choices we want, and the punishments that would stop them from making choices we do not want. For instance, would warning messages when connected to fast unsecure Wi-Fi encourage employees to switch to slower but more secure Wi-Fi?

For *understanding mapping* between available options and consequences that follow, we need to be aware of the risks employee's take and the convenience employee's gain. For instance, studies looking at choosing between more secure Wi-Fi not protected by password and less secure Wi-Fi protected by password shows that people have a prejudice towards more secure solutions being more complex by default, and less secure solutions being easier and faster to implement [24].

Choices provided by *default* have shown to be selected by people who hesitate about choices, do not understand them or do not pay much attention to them. Software development companies noticed this, and most software installations have default settings. Similarly default choices for security-related decisions may be pre-selected to the most secure, leaving the freedom for users to uncheck selections or change defaults if desired.

Giving feedback on choices, whether they were positive or negative, helps users to learn from their past decisions and use this experience in future. Knowing that users make errors and *expecting errors* means being more creative in providing available choices in a simple and understandable manner, as well as guiding choices with explanations and help options. The last point is also important for helping with presentation and *structuring of complex choices* to reduce people's cognitive loading, e.g., sectioning decision so that there are clear steps and a limited number of options to choose from at any point in time [25].

In addition to the six influencing techniques provided, organizational psychology and behavioural economics supply other ways to influence people's behaviour, one of which is MINDSPACE. The MINDSPACE framework [26] highlights influencing techniques some of which are common to those presented in [22]: messenger, incentives, norms, default, salience, priming, affect, commitment and ego. *Messenger* indicates the owner of the recommendation, e.g., boss of the company and *norms* appeal to choices other people in society or company are doing. *Salience* emphasizes how the choice is important to us. *Priming* addresses framing effects, which is related to our subconscious, and *affect* appeals to our emotional component. *Commitment* refers to our promises made and *ego* appeals to acting in a way that makes us feeling good about ourselves. Similarly to nudges, influencing factors can be used for constructing choice architectures in security. In addition, [27] outlines a process by which companies can explore the creation of nudges to solve specific security problems within their companies by using MINDSPACE as part of creative workshops with staff.

3.2.3. Nudging for security and productivity: When is it appropriate?

The company may decide on when to apply nudging depending on the level of control the company has over the device. Recalling Table 3 with four various cases of device ownership and management, resulting in three levels of control: full, partial and no control. Taking into account possible context in which the security related decisions are made, here, we argue on appropriateness and benefit of nudging, see Table 4. Similarly to Table 3, we consider the owner and manager of the device (company or employee) and context (working or not, e.g. public places, home, private houses, other companies). In Table 4 in 'Nudging' column '+' and '-' indicate cases, where nudging is desirable and beneficial and not, respectively.

Table 4. Devices control and nudging

#	Device Owner	Device Manager	Context	Control	Nudging
(1)	Company	Company	Working	Full	-
(2)	Company	Company	Public/Private	Partial	+
(3)	Company	Employee	Working	Partial	+
(4)	Company	Employee	Public/Private	Partial	+
(5)	Employee	Company	Working	Partial	+
(6)	Employee	Company	Public/Private	Partial	+
(7)	Employee	Employee	Working	Partial	+
(8)	Employee	Employee	Public/Private	No	-

Note that in the *context* we can also include services that the employee is allowed to use. For instance, in case publicly available services are used by employees at work on working devices, such as Dropbox or social networks, the scenario should no longer be classified as the first case of full control.

Indeed, with the exception of case (1) of full control, where a company controls and manages working devices in working context, and case (8) of no control, where there is no any control over an employee's owned and managed device used in non-working context, presented in Table 4, nudging is appropriate and beneficial in the rest of the cases of partial control over a device.

For instance, an Information Security policy may state that users should not access social networks from a work device. A company may restrict access to such a websites and prevent access in case (1). However, that would not be possible in case (3), where an employee is managing corporate device, or in case (6), where an employee works on a personal device providing some managing privileges to the company, and such a restriction would disturb employee's ownership feelings. On the contrary, nudging employees away from social networks websites during working hours would be seen as advice from the company that an employee can override when justified, e.g., for working purposes in order to advertise some company products or jobs in social networks.

3.2.4. Nudging for security and productivity: Examples of scenarios

Nudging has being applied to information security, for instance, for framing users against making privacy invasive choices [5-8]. Changing colour may also affect our perception of available options, for instance, traditionally, red is associated with danger, e.g. red in traffic light or famous 'red button', and green with safety or 'to go' in a traffic light signal. Therefore, traffic light colour schemes are widely applied in cyber security design, e.g., for indicating what can be done with shared information in a traffic light protocol [28] or for framing choice options [5].

The first experiments on applying nudging in the security context of a public Wi-Fi selection are presented in [8], [11]. In this works an example of nudging a user towards selecting a more secure Wi-Fi is considered. Choice architecture is organised so that available Wi-Fi's are ordered in such a way that the most secure networks are placed at the top of the list and their names are painted in 'green', while names of less secure Wi-Fi's are painted in 'yellow' and open Wi-Fi's in 'red'. The results show that the colour was effective in influencing the choice of users, when compared to the order, which did not change the choice significantly. However, in preliminary evaluations the combination of order and colour successfully nudged more people away from insecure networks than one factor alone.

4. Conclusions

In this work, we have discussed the recent trend of both large companies and SMEs towards adopting the consumerisation of IT. In addition to the commonly recognized risks and opportunities that this trend carries for the companies and their employees, we highlighted the uncertainty that consumerisation introduces. This uncertainty is due to the changed ownership model and context or the potentially unsecure environments, in which an employee is using private or company owned devices and corporate data. To help mitigate against potential risks, we have suggested the adoption of a 'soft' strategy of nudging that tries to influence the choices of employees by subtly pushing them towards more appropriate decisions, leaving the final choice and the responsibility for its consequences to employees. This approach can be used to complement the company's compliance policy. In addition, such an approach takes into account the ownership model and considers the dynamics of the context, in which employees might be in a better position to make a decision.

When compared to a more restrictive and less flexible compliance policies, which leave no choice to decision makers, an alternative 'soft' nudging approach looks appealing when freedom of choice is at stake. This approach pushes users towards more responsibility, when dealing with corporate data/device, which may also be advantageous, considering awakening awareness of employees with regards to security risks.

As future work, we are considering development of rigorous risk assessment of trade-off solutions for concrete security scenarios to ground solutions towards which nudging is performed. It is a complex task of trading security and productivity objectives of a decision maker, while taking into account security policy of the company and the employee's personal preferences. We also aim at proposing methodology to construct choice architectures in security, and to be able to evaluate the impact in corporate risk through nudging techniques.

Acknowledgements

The authors acknowledge funding for "Choice Architecture for Information Security" (ChAISe) project EP/K006568/1 from Engineering and Physical Sciences Research Council (EPSRC), UK, and Government Communications Headquarters (GCHQ), UK, as a part of Cyber Research Institute. We would gratefully acknowledge the support and contribution of our colleagues on the ChAISe project from Northumbria University: Debora Jeske and Pam Briggs, who worked with us to identify issues and solutions in this project.

References

[1] Consumerisation: The Power of Many. Economist, Special Report: Personal Technology, 2011, Available online: [http://www.economist.com/node/21530921].

[2] Trend Micro Inc. Trend Micro Helps IT Embrace Consumerization; Computer Security Update 12(8) 2011. Available online: [www.wvpubs.com].
[3] Hanks AS, Just DR, Wansink B. Trigger foods: The influence of irrelevant alternatives in school lunchrooms. Agricultural and Resource Economics Review, 41(1); 2012, p.114-123.
[4] Applying behavioural insights to reduce fraud, error and debt, Behavioral Insight Team. Cabinet Office report, UK 2012. Available online: [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60539/BIT_FraudErrorDebt_accessible.pdf].
[5] Choe EK, Jung J, Lee B, and Fisher K. Nudging people away from privacy invasive mobile apps through visual framing. In INTERACT, LNCS, Springer. 8119 (3); 2013, p. 74-91.
[6] Wang Y, Leon PG, Scott K, Chen X, Acquisti A, Cranor LF. Privacy nudges for social media: an exploratory Facebook study. In Proceedings of the 22nd international conference on World Wide Web companion (WWW '13 Companion). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, 2013; p. 763-770.
[7] Acquisti A, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy, 7(6); 2009 p. 82-85.
[8] Turland J, Coventry L, Jeske D, Briggs P, Laing C, Yevseyeva I, van Moorsel A. Nudging towards security: Developing an application for wireless network selection for android phones. (in preparation)
[9] Morisset C, Gross T, van Moorsel A, Yevseyeva I. Nudging for quantitative access control systems. In Human Aspects of Information Security, Privacy and Trust, HCII. Springer, 2014, (to appear).
[10] Morisset C, Yevseyeva I, Gross T, van Moorsel A. Formalization of Nudging in Information Security. 11th International Conference on Quantitative Evaluation of SysTems (QEST 2014), (submitted).
[11] Jeske, D., Coventry, L., Briggs, P., & van Moorsel, A. (2014). Nudging whom how: IT proficiency, impulse control and secure behaviour. CHI Workshop on Personalizing Behavior Change Technologies, CHI 2014. Available online: Available online: [http://personalizedchange.weebly.com/1/post/2014/03/nudging-whom-how-it-proficiency-impulse-control-and-secure-behavior.html]
[12] Tech Dep of ENISA Section Risk Management and Patsis G (Obrela Security Industries). Information Package for SMEs with risk assessment / risk management for two SMEs. ENISA report 2007. Available online: [https://www.enisa.europa.eu/activities/risk-management/files/deliverables/information-packages-for-small-and-medium-sized-enterprises-smes].
[13] BS ISO/IEC 27005:2011 British standard for Information technology – Security techniques – Information security risk management. BSI standards Publication. 2011.
[14] Clarcke J, Hidalgo MG, Lioy A, Petkovic M, Vishik C, Ward J. Consumerization of IT: Top risks and opportunities. Responding to the evolving threat environment. ENISA report 2012. Available online: [http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/consumerization-of-it-top-risks-and-opportunities].
[15] Clarcke J, Hidalgo MG, Lioy A, Petkovic M, Vishik C, Ward J, Marinos L. Consumerization of IT: Risk mitigation strategies. Responding to the evolving threat environment. ENISA report 2012. Available online: [http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COITMitigationStategiesPublishedVersion.pdf].
[16]Thompson HH. Consumerization and security: Effective Security Practice Series. Microsoft Corp. White paper. 2010. Available online: [download.microsoft.com/download/E/F/9/EF9F24B7-DB49-44D4-8F6A-A49D5020B8B8/Consumerization_Final.pdf].
[17] MWR Infosecurity and CPNI. Mobile Devices Guide for Implementers. 2013.
[18] Hunt J, BYOD Policy – What Businesses Need to Consider, Credit Control, 2012; 33(5/6), p. 69.
[19] Savage M, IT consumerization drives new security thinking. Information Security Magazine, 27 May 2011 Available online: [SearchSecurity.com].
[20] Beautement A, Sasse MA, Wonham M. The compliance budget: managing security behaviour in organisations. In Proceedings of the 2008 workshop on New security paradigms (NSPW '08). ACM, New York, NY, USA, 2008; p. 47-58.
[21] Kirlappos I, Parkin S, Sasse MA. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. In Proceedings of Workshop on Usable Security, 2014.
[22] Thaler RH and Sunstein CR. Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven, CT, USA: Yale University Press; 2008.
[23] Fletcher A, Marteau T, Worsley T. Helpdesk report: Use of behavioural economics in development interventions, 2012. Human Development Resource Centre. Available online: [http://www.heart-resources.org/wp-content/uploads/2012/05/Use-of-Behavioural-Economics-February-2012.pdf]
[24] Kim BC, Park YW, Security versus convenience? An experimental study of user misperceptions of wireless Internet service quality, Decision Support Systems, 53 (1); 2012, p. 1-11.
[25] Miller, GA. The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review 63(2);1956, p. 81–97.
[26] Dolan, P., Hallsworth, M., Halpern, D., King, D., & Metcalfe, R. Influencing Behaviour: The MINDSPACE way. Journal of Economic Psychology, 33, (2012) 264-277.
[27] Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cybersecurity Environment. In Design, User Experience, and Usability. HCII. Springer, 2014, (to appear).
[28] Farnham G, Leune K. Tools and standards for cyber threat intelligence projects, 2013.